CHAPTER 6

CONCLUSIONS

6.1 Introduction

Spam filtering has been studied numerously since its emergence. This process is only limited to distinguish between valid and spam messages. Many of studies also related to spam clustering which basically to group spam messages based on its content. However, assessing the risk level of a spam message is acknowledged to be a rare study in research world since the only minimal amount of publication found for the related works at the time of this writing. The study of measuring the hazardous impact is widely carried out in the field of intrusion attack and virus outbreak.

Motivated by this sparseness and the intention to assist users to decipher the implicit risk of text spam messages, this study aims to investigate possible solution in measuring the hidden risk by application of the Danger Theory.

This chapter elaborates the simplification of the methodology applied and the findings gathered from the experiments. Some implications for future research and potential contribution to the knowledge also discussed at the end of this chapter.

6.2 Contribution

The issue of not knowing the impact that might cause by spam due to lacking awareness among users of the potential loss has become motivation for this study. Determine to produce a possible comprehensive solution, the research objectives are established as the following:

i. to study and evaluate the Danger Theory of AIS for application in risk identification and assessment on text spam messages;

ii. to propose and develop a model that is related to the assessment of spam risk level using an integration of the Danger Theory, text mining and risk assessment methodology; and

iii. to evaluate the accuracy of the proposed model with the aim of more than 90% accuracy rate.

Chapter 2 has reviewed the spam evolution since its emergence from the perspective of spam's format, characteristics and also a divergence of spam intention. The first objective is validated in this chapter. The reaction of users or human behaviour towards online threat is found as easily get enticed with the unknown source of messages. This is affirmed by numerous reports and statistics of loss. Available mechanism of controlling spam also has been identified and some deficiencies are recognized to be solved via this study. Realizing that there is similarity of dendritic cells behaviour defending the body from any harm in the field of spam management, Danger Theory from AIS is applied in developing the solution. Designation and development of the risk assessment for spam are inspired on how these cells scan their surroundings to detect any anomaly situation. The recognition of antigen and the signals processing has been applied in this risk assessment study. The concept of text mining also has been applied and impressively demonstrated to be set as antigens and signals derivation.

The second objective of the study is validated in Chapter 3 and 4 of the thesis. In Chapter 3, the model of risk assessment is designed and developed based on identified properties in Danger Theory and text mining. The biological abstraction from Danger Theory is mapping with the spam risk assessment model. The model is established as a medium that able to categorize the risk level based on its calculated risk concentration. The content of messages is treated as the context for assessment. This proposed solution is known as Risk Concentration for Context Assessment or RiCCA. Text mining concept such as weighting schemes and pre-processing are applied to process the text messages at the initial stage. This context then is further assessing by DCA and dDCA, algorithms of Danger Theory. The public dataset of SMS messages from UCI Machine Learning Repository is deployed as groups of antigen.

Identified properties are subsequently considered in Chapter 4 as prospect characteristics for the algorithm. This algorithm is visualized and transformed into prototype formation. The prototype is intentionally developed to execute the experiments in a larger size of data and for faster assessment that is elaborated in Chapter 5. Moreover, this prototype can be further enhanced as a potential mobile

application for users as a tool to eliminate inherent dangerous spam. The prototype is depicted in the format of the diagram, process flow, and pseudo-code.

A series of the experiment is conducted to examine the reliability of RiCCA, the proposed algorithm in assessing the risk level of spam messages. This is elaborated in Chapter 5 and the performance of the proposed solution is justified. The experiments are executed using the developed prototype and two different sources of data are merged and deployed as the antigens population. The final objective of the study is verified by measuring the performance of RiCCA to distinguish spam messages and categorized according to its malicious status.

In this study, the final outcome of the research is a prototype developed computationally. This prototype is beneficial to execute the testing in an automated way and to potentially reduce the total time taken in measuring the risk; compared to if the testing is conducted manually. This developed prototype comes in handy especially when the testing is executed with a large size of dataset and will shorten the time taken in completing the testing.

In addition, this study has its distinctive findings that contributed in the field of spam management. They are identified as the following:

6.2.1 Application Of Danger Theory In Risk Measurement

Application of the Danger Theory in information security risk assessment is the novel feature of this study. The nature of Danger Theory to detect malicious surroundings commonly and numerously applied and limited only in filtering anomalies. This study has demonstrated that Danger Theory is a reliable and feasible theory to be applied in detecting a malicious substance to an extended function that is measuring the severity level potentially caused by the malicious entity. The biological properties have been articulately mapped with the characteristics of spam in its management. Throughout the experiments, the risk for unknown messages is calculated by processing the antigens and its associated signals.

This study has enhanced the concept of Danger Theory in measuring risk concentration quantitatively (translated in numerical value) through identification of the reliable term weighting scheme in text classification.

Previous research that considers content of messages as methodology is enhanced with this study where the content (term) is assigned with the weight value statistically to indicate its malicious intensity.

6.2.2 Significant Role Of Text Mining

Text mining is prominently applied to extracts the useful information and knowledge hidden in the text content. This process has been applied in this study to set the pre-determined value of weight for every term exists in the context. Pre-processing in mining the text is used to reduce the noise which is usually referring to unwanted or meaningless term. With text mining, every term that is considered as an antigen is able to derive its weight value that reflected the signals concentration. These antigens and signals item attain the pre-requisite of Danger Theory functions. The effect of pre-processing has been verified throughout this study.

6.2.3 Full Cycle Of Spam Management

The threat is critically required to be managed. Spam that is recognized as one of the online threat has its own risk that potentially leads to impact loss if it is not well managed. There is various of standards for risk management that has been established. All risk management basically consists of four (4) main steps; risk identification, risk assessment, response and treatment of risk, and the final step are risk monitoring. The existing spam management only consists of spam filtering which has been studied numerously by other researchers. Until recently, there is no appropriate action taken to assess the severity of spam. Nevertheless, there are records and statistics available for documenting the losses caused by spam. This study somehow illustrated the importance of assessing the severity level of spam and how to respond appropriately. Through this study, the cycle of risk management has been completed with the assessment of risk.

6.2.4 Implicit Risk Reader For Users

With the development and implementation of this study, the proposed model can be a medium in helping users identify the danger or damage that may cause them by SMS messages. Scam and fraud that are widely spread via SMS messages nowadays can be detected at early stage and impact may be avoided. Hence, users' decision can be intervened with this implicit risk reader.

6.3 Limitations

Throughout this study, there are limitation and drawback identified. One of the apparent elements is the algorithm itself. DCA has too many parameters to be considered that caused it is very hard to achieve high accuracy detection rate. A slight or minimal change in one parameter value could cause the final calculated outcome highly deviates from the initial expectation.

The issue of weight sensitivity also is needed to be arranged carefully when deploying DCA as a classifier. Slightly change in value may cause DCA producing high false positive or false negative rate.

For this specific study, text mining has contributed mechanism for antigen and the derivation of the signal value for DCA. However, its database list such as stop word list and root word list must be always be updated. Inadequate content of these lists affected the algorithm to perform well in achieving high accuracy detection rate.

Although there are drawbacks in DCA, it is not impossible to further examine in finding a solution for optimizing the output produced by this algorithm.

6.4 Future Research

There are various potential aspects that can be taken seriously for the future research, which includes the following:

6.4.1 Automate As Mobile Application

The prototype developed as elaborated in Chapter 4 is potential to be developed as a mobile application. This may benefit users by assisting them to identify the severity of unknown messages. Other than that, advanced mobile

applications can be developed to verify the claimed performance in a mobile platform such as Android and IOS. It also is expected in helping users to respond such as eliminate the message or even escalate such disturbance message to authority body, for instance, SKMM in Malaysia. This mobile application can be further verified for its reliability and consistency in distinguish spam and differentiate its risk level.

In addition to the current metrics for performance, the total time taken (in seconds) is also suggested as one of the evaluations. Since DCA performs linear calculations for its computation, making the system low weight theoretically. This can be further tested and executed in mobile application form. The shorter the time taken (CPU time) to process the spam message for its severity level, the better the model it is.

6.4.2 Extended Scope Of Spam For Testing

Even though this work is successfully realized in assessing severity concentration of a limited text message (SMS with 160 characters), it is anticipated that this proposed solution to be extended to test with various type of spam and with unlimited context size. Since spam is prominent in many formats, this is foreseen as possible to be further tested. In addition to that, the unknown malicious status of messages can be tested in another language.

6.4.3 Enhancing The Data Availability

Throughout this study, it is a struggle to find another set of data to be tested. Even though there are online and shared dataset available, it is always beneficial if another set of data is available too. The test can be expanded in many ways and the availability of data is crucial for this study. Future study may deploy another set of data hopefully to be in larger size and can be shared with other researchers.

6.4.4 Comparative Analysis With Other Technique

There are always comparison and competition between immune and non-immune algorithm. Researcher s always claimed one kind is better than another in their findings. The developed algorithm can be further analysed and compare with another classifier just to find a better solution for this problem.

6.4.5 Other Fields Of Research

This works somehow potentially could initiate a further study for other text mining fields especially in computational linguistics. Furthermore, the application of Danger Theory also intentionally stimulates another field of risk assessment, besides current work in malware and intrusion detection.

6.5 Summary

Spam distribution will not be able to totally vanish. It will always be evolved together with the technology advancement. However, countermeasures are needed to dwindle away this issue and also to lessen its impact loss. Awareness among users must be timely updated with the information for spam latest platform, mechanism of distribution and also implicit intention. The effort to curb this issue must be promoted continuously and aligned with the spam evolution and technology advancement. Besides users' discretion, intervention from some tool may help them in making decision, especially which involved information security. The major contribution of this thesis is the development and implementation of Danger Theory in measuring risk. The experiments has demonstrated that the model developed from this theory is feasible computationally. In this thesis, the Danger Theory is successfully applied to the classification of risk level for SMS messages.